

روش های کلاه برداری در دنیای ارز دیجیتال که تا حالا نمی دانستید!

Scam Methods in Cryptocurrency



7 روش متداول کلاه برداری در دنیای ارز دیجیتال که باید همین الان بدانید!

آیا شما هم از کلاه برداری در دنیای ارز دیجیتال مطلع هستید؟ افرادی که در این فضای نوین فعالیت می کنند، از شنیدن اخبار کلاهبرداری های مختلف در دنیای ارز دیجیتال خسته شده اند. هر چند در این دنیای جدید کلاهبرداری های بزرگ و مختلفی انجام شده، اما نمی توان به تمامی ارزهای دیجیتال به عنوان صنعتی غیرقابل اعتماد نگاه کرد.

این امر نشان از ناآگاهی افرادی دارد که برای درک بیشتر و آشنایی با این انقلاب جدید، هیچ تلاشی نکرده اند. همان طور که گفتیم، به طور حتم کلاهبرداری هایی در دنیای ارزهای دیجیتال اتفاق افتاده، اما این اتفاق در تمامی صنایع و حوزه ها اتفاق می افتد. با تکیه بر این امر، می خواهیم 7 روش متداول کلاه برداری در دنیای نوین ارز دیجیتال را در این مقاله از کیف پول من آشکار کنیم.



متداولترین روش کلاه برداری در دنیای ارز دیجیتال توسط عرضه اولیه سکه اتفاق می افتد. افراد با ایجاد فضایی پرشوق و پرهیجان برای عرضه اولیه ارزها، از این راه به کلاه برداری می پردازند. به دلیل این که عرضه اولیه ارز یکی از بهترین راهها برای ایجاد یک پروژه، نوآوری در جمع آوری سرمایه برای ایجاد پروژه است، اغلب از این کار سوءاستفاده می شود.

بلاک چین اتریوم به بستر مناسبی برای انجام کلاه برداری توسط عرضه اولیه تبدیل شده، اما این کارهای غیرقانونی را نمی توان گردن بلاک چین اتریوم انداخت؛ چرا که اتریوم مسئول پروژه ها و برنامه های متن باز اکوسیستم خود نیست.

مطلب پیشنهادی : [هارد کپ چیست؟](#)

در عوض، کلاه برداری‌های انجام شده تقصیر افراد تازه وارد حوزه ارزش‌های دیجیتال است که قصد دارند با هولد کردن کوین‌ها، در عرض یک شب 100 برابر سود کنند. متداول‌ترین نشانه‌هایی که می‌توانید عرضه اولیه ارزش‌های نامعتبر را شناسایی کنید بدین شکل است:

- وایت پیپر کپی شده
- افراد ناشناس تیم سازنده
- عجله در اجراسازی پروژه
- متغیر بودن صحبت‌های گفته شده و نوشته شده روی وایت پیپر
- جواب ندادن به سوالات اصلی و پیچیده
- دلیل ضعیف برای اقتصاد توکن
- نبود نقشه راه

در خرید عرضه اولیه ارزش‌ها بهتر است به تمامی جنبه‌ها و اطلاعات موجود آن ارز و تیم سازنده نگاه کنید و با در نظر داشتن احتمال کلاه برداری، همه سرمایه خود را تنها وارد دنیای یک ارز دیجیتال نکنید.



دومین شکل متداول کلاه برداری که ممکن است در دنیای ارزهای دیجیتال با آن مواجه شوید، صرافی‌های مشکوک هستند؛ صرافی‌هایی که یک شبه معروف شده و شروع به تعریف از خود می‌کنند. افراد باید در استفاده از چنین صرافی‌هایی محتاط عمل کنند؛ چرا که اگر ارزهای خود را در این صرافی‌ها وارد کنید و قصد صرافی کلاه برداری باشد، هیچ راهی برای برگشت سرمایه خود نخواهید داشت.

این مورد حتی برای صرافی‌های معتبر نیز قابل تعمیم است. صرافی‌هایی که طی زمان اعتبار کسب کرده‌اند، اما نتوانسته‌اند در طول زمان سرمایه خوبی جذب کنند و از بازار عقب مانده‌اند، می‌توانند در کمین ارزهای شما باشند. تعدادی از صرافی‌های معتبر خارجی که این عمل را انجام داده‌اند به شرح زیر هستند. [crypto01](#)، [btc-cap](#)، [capital-coins](#)، [coinquick](#)، [cryptavenir](#)، [crypto-banque](#)، [crypto-infos](#)، [cryptos.solution](#) و غیره تعدادی از صرافی‌های کلاه برداری خارجی دنیای ارز دیجیتال هستند.

کیف پول‌های قلبی

با عرضه [ارز دیجیتال بیت کوین](#)، کیف پول‌های قلبی زیادی برای سیستم عامل اندروید در پلی استور منتشر شد؛ به همین خاطر توصیه می‌کنیم به هیچ وجه از کیف پول‌های نامعتبر و تصادفی در پلی استور استفاده نکنید. این کیف پول‌ها می‌توانند قلبی بوده و هر لحظه سرمایه شما را بدزدند.

هرچند چنین کیف پول‌هایی ادعا می‌کنند که به طور کامل می‌توانید کنترل دارایی‌های خود را به دست بگیرید، اما بهتر است بدون دقت لازم از کیف پول‌های مختلف استفاده نکنید.

چنین اعمالی در دنیای ارز دیجیتال رایج شده و به طور معمول در هنگام [فورک‌های بیت کوین](#) اتفاق می‌افتد. در صورتی که در تله این افراد بیفتید، بیت کوین‌های خود را نیز از دست خواهید داد. هرچند اپ استور اپل به عنوان فروشگاه معتبر و مطمئن شناخته می‌شود، اما در این فروشگاه نیز تعدادی برنامه قلبی وجود دارد.

یکی از افراد فعال در حوزه ارزهای دیجیتال با چنین اتفاقی مواجه شد. به گفته وی، او وارد اپ استور شده بود تا با دانلود یکی از برنامه‌های کیف پول به بررسی سرمایه بیت کوین خود بپردازد.

وی پس از نوشتن نام برنامه، یکی از برنامه‌ها را دانلود کرده و اطلاعات خود را وارد می‌کند. پس از گذشت چند دقیقه، حساب وی خالی می‌شود. او پس از بررسی برنامه مطلع شده که لوگو و آیکون برنامه با کیف پول اصلی متفاوت بوده و 17.1 بیت کوین خود به ارزش 600 هزار دلار را از دست داده است.

طرح‌های هرمی یا پانزی

هرچند این نوع از کلاه برداری بسیار راحت شناسایی می‌شود، اما همچنان افراد در تله تیم‌های کلاه برداری می‌افتند. اگر با ارز دیجیتال یا پروژه‌ای مواجه شدید که برای افزایش و چند برابر کردن سرمایه، درخواست عضو گیری و دعوت از اعضای جدید را دارد، با [طرح پانزی](#) روبرو هستید. همچنین طرح‌هایی که وعده برگشت سرمایه چند برابر را می‌دهند نیز از طرح‌های مختلف پانزی هستند.

با یک آزمون نمایانگر می‌توانید از حضور در پروژه‌ها و طرح‌های هرمی جلوگیری کنید. آنتونوپولوس برای شناخت چنین طرح‌هایی، دو راهکار ساده پیشنهاد می‌دهد. آیا پروژه قول برگشت سرمایه منظم بیشتر از انتظار بازار را می‌دهد؟ آیا پروژه بیشتر روی جذب افراد جدید تمرکز دارد تا روی محصول نهایی؟ در هر دو حالت با طرح پانزی روبرو خواهید بود.

مطلب پیشنهادی : [اصطلاحات تخصصی ارز دیجیتال](#)

کلاه برداری با فیشینگ

فیشینگ یکی از رایج‌ترین روش‌های کلاه برداری در دنیای ارزهای دیجیتال و دیگر حوزه‌های اینترنت است که افراد به سادگی در دام آن می‌افتند. افراد با دریافت نام کاربری، رمز عبور و کلید خصوصی کیف پول شما سرمایه‌تان را می‌دزدند. اکثر این افراد با دو روش متداول زیر فیشینگ را انجام می‌دهند:

- ایردراپ تقلبی
- Punycode

گروه‌های پامپ و دامپ

گروه‌های پامپ و دامپ در برنامه‌های تلگرام، اسلک و دیگر برنامه‌ها، مورد تازه‌ای در بازارهای سنتی نیستند. دنیای ارز دیجیتال نیز از قاعده عقب نمی‌ماند و گروه‌های پامپ و دامپ خود را دارد. اگر در برنامه تلگرام جستجو کنید، با گروه‌هایی به جمعیت 40 الی 100 هزار نفری مواجه خواهید شد.

به نظر شما در این گروه‌ها چه اتفاقی می‌افتد؟ چنین گروه‌هایی برای صحبت‌های ساده طراحی نشده‌اند، در عوض افراد برای تغییر [قیمت ارزهای دیجیتال](#) آلت کوینی که مارکت کپ پایینی دارند استفاده می‌کنند.

در این شرایط افرادی که سریع عمل کنند سود کرده و افرادی که کمی تاخیر داشته باشند، با کاهش شدید قیمت‌ها مواجه می‌شوند و ضرر زیادی می‌کنند. ابزارهای مختلفی طراحی شده‌اند تا به راحتی با اندازه‌گیری حجم بازار، چنین طرح‌های کلاه برداری را شناسایی کنید.

جعل هویت

یکی از مصنوعی و غیرطبیعی‌ترین روش‌های کلاه برداری در دنیای ارزهای دیجیتال، جعل هویت است. در این روش از کلاه برداری، افراد حساب‌های کاربری فیک در توییتر و فیسبوک ایجاد می‌کنند. افراد با جعل هویت شخصیت‌های واقعی و پشت صحنه یک پروژه سعی دارند تا به کلاه برداری بپردازند.

اگر سری به توییتر بزنید، با افراد متعددی مواجه می‌شوید که خود را به جای یکی از افراد شناخته شده در دنیای ارز دیجیتال جا می‌زنند و خبر از انتشار توکن‌ها و ایردراپ‌های جدید می‌دهند. همچنین، برخی افراد به عنوان تیم پشتیبانی **صرافی‌های ارز دیجیتال** نیز فعالیت می‌کنند تا سرمایه شما را از چنگتان درآورند.

از کلاه برداری‌های ارز دیجیتال مطلع باشید!

کلاه برداری در تمامی صنایع اتفاق می‌افتد و ارز دیجیتال که به سمت غیرمتمرکز و متن باز بودن پیش می‌رود، بستری مناسبی برای کلاه برداری است. تنها راهی که می‌توانید از کلاه برداری جلوگیری کنید، تکیه به منابع معتبر و دانش شخصی است. با مطالعه اخبار و مطالب منتشر شده در منابع معتبر می‌توانید اطلاعات زیادی به دست آورید.